The 9th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 14th 2014

INTERCEPTION OF COMMUNICATIONS MADE OVER THE INTERNET IN ACCORDANCE WITH THE PROVISIONS OF THE CODE OF CRIMINAL PROCEDURE

Ungureanu Petre PhD Candidate
„Aexandru Ioan Cuza" Police Academy
Aleea Privighetorilor, nr. 1-3, Sector 1, Bucharest, Romania

Abstract
By interception of communications we refer to interception, access, monitoring, gathering and recording of communications made by means of telephone, informatics system or any other such means. The article tries to describe the legal framework of interception of communications made by use of internet based applications, such as Facebook, Yahoo, Gmail, Skype, What's Up, Viber, Tango, Twitter.

Keywords:
Interception, technical surveillance warrant, informatics system, communications, Internet, applications, Romanian Intelligence Service,

1. Regulations in the field of interception and audio recording

Regulations regarding the interception and recording of audio and video found in Romanian legislation in:
- Romanian Code of Criminal Procedure
- Romanian Criminal Code (offenses provided in Article 226: ,,invasion of privacy", Article 302:,,violation of secret of correspondence", Article 324: "Falsification of technical Register", Article 361: Illegal interception of computer generated information.
- Law No 51/1991 on Romania's national security.
- Law No 535/2004 on preventing and combating terrorism.
- Law No 191/1998 the organization and functioning of the Security and Protection Service
- Law No 143/2000 Law against illicit drug trafficking
- Law No 678/2001 on preventing and combating trafficking in persons
- Law No 39/2003 on preventing and combating organized crime.
- Law No 656/2002 on preventing money laundering
- Law No 78/2000 on preventing, discovering and sanctioning corruption
- Law No 64 / 2004 for putting in effect the Council's of Europe Convention on Cybercrime
- Law No 591/2002 - Law approving Government Emergency Ordinance No. 79/2002 on the general regulatory framework for communications.
- Law No 506/2004 the processing of personal data and privacy in the electronic communications sector.

In the current Criminal Procedure Code, entered into force on 01.02.2014, legislator limited special surveillance or research methods to Article 138:

INTERCEPTION OF COMMUNICATIONS MADE OVER THE INTERNET IN ACCORDANCE WITH THE PROVISIONS OF THE CODE OF CRIMINAL PROCEDURE

- Interceptions of communications or any type of remote communications
- access to a computer system
- Surveillance by video, audio or photo methods
- Localization and tracking by technical means
- Obtaining data on financial transactions of a person
- Retaining or search of correspondence
- Use of undercover investigators and collaborators
- Authorized participation to certain activities
- Controlled delivery
- The obtaining of data generated or processed by providers of public electronic communications network or by providers of publicly available electronic communications, other than the contents of communications, withheld under the special law on the retention of data generated or processed by providers of public electronic communications networks and providers of public electronic communications networks and providers of publicly available electronic communications.

Technical supervision may be ordered for offenses against national security under the Penal Code and other special laws, as well as the offenses of drug trafficking, arms trafficking, trafficking in persons, terrorism, money laundering, counterfeiting or other assets, falsification of electronic payment instruments, against property, blackmail, rape, deprivation of liberty, tax evasion, corruption offenses against the financial interests of the European Union, offenses committed by means of electronic communications systems and for other offenses for which the law provides for punishment imprisonment for five years or more.

Art. 138 specify conditions which may provide technical supervision, which must be met cumulatively, namely:

- a reasonable suspicion about the preparation or commission of an offense referred to in Article 139 paragraph 2 of the Criminal Procedure Code (listed above)
- The measure must be proportional to the restriction of fundamental rights and freedoms, given the particularities of the case, important information or evidence to be obtained or the seriousness of the offense.
- Evidence could not be obtained in any other way or would require special difficulties in obtaining the evidence which could prejudice the investigation or there is a threat to the safety of persons or property value.

Technical surveillance is authorized by the rights and freedoms judge of the court which would return jurisdiction to hear the case in the first instance or the instance corresponding to its level in whose jurisdiction the headquarters prosecution of which the prosecutor made the request.

2. Interception of communications or any type of remote communication

According to Article 138, paragraph 2 of the Criminal Procedure Code by intercepting communications or any type of communication means interception, access, monitoring, collection and recording of communications by telephone, computer system or by any other means of communication.

With the help of technical means on one hand are captured and taken under control private conversations or communications made by telephone, computer system or other means of communication by one person and, on the other hand, all intercepted call or communications content are stored for later processing or analysis. All systems, devices

and equipment that are necessary for intercepting communications are called "operative technique".

2.1. Interception of communications made over the Internet via Facebook, Yahoo, Gmail, Skype, What's Up, Viber, Tango, Twitter is subject to specific regulations stipulated by Article 138, paragraph 1, letter a of the Code of Criminal Procedure.

Below we present some of the existing IT applications on the Internet that allow communication of audio, video or messaging type that may be subject to technical supervision in accordance with the Code of Criminal Procedure.
Facebook is currently one of the most used applications on the internet. It is a social network, thus to person who uses it is assigned a user name and password after your completed application for registration.
Yahoo provides the following services: Yahoo Mail, Yahoo Messenger, Yahoo Answer, Yahoo Video, Yahoo Directory, Yahoo News, Yahoo Finance, Yahoo Groups, Yahoo Maps.
Yahoo Mail is a web mail service. To access this service, the creation of an account with a personal password is required.
Yahoo Messenger is an instant messaging service. Access to this service requires a computer program to enable access to this service, based on an assigned Yahoo account.
Google is the most used search engine on the internet and provides help to any user for finding information on the web. Also provides services like Google Earth (satellite images of Earth recorded), Google Chromium (web browser), Android operating over system for mobile, Gmail, email service.
Google talk it's an instant messaging service and Google+ is a social network.
Skype - is free software that allows Internet users to communicate via video with other Skype users. Currently this application is owned by Microsoft.
What's App Messenger is an instant messaging service used for mobile phones: Nokia, iPhone, BlackBerry, Android and allows you to send messages without paying SMS.
Viber is an messaging application used for mobile phones. Users can communicate through this application both by voice and by text.
Twitter is actually a website that allows the transmission of messages by internet users.
Tango - is a software application that once installed on computers or mobile phones enable communication between users. The condition is the creation of an account and the registration as a user.
All these applications allow communication between users. In case these applications are used for preparing or committing crimes warrants for technical surveillance can be obtained.
Regarding use of such warrants few remarks need to be made. Currently the institution that implements the technical surveillance warrants that concern intercept communications or any type of communications or remote access to a computer system is the Romanian Intelligence Service (R.I.S.).
Romanian Intelligence Service is authorized by law to administer the National Center for Interception of Communications (CNIC). Romanian Intelligence Service provides technical support for putting in effect surveillance warrants obtained by other services like Directorate of Special Operations of Romanian Police Department and Directorate of Information and Internal Affairs, National Directorate of Anticorruption.

Technical problems arise when we deal with surveillance warrants that involve communications conducted via the internet using Google Apps, Gmail, Google Talk, Facebook, Yahoo mail, Yahoo messenger, Twitter, Skype, mobile terminals or applications like What's App Messenger, Viber, Tango. In this case, in order to successfully put in effect surveillance warrants some solutions can be found:

- Romania should draft cooperation treaties with the States that host the central servers of these applications, in order to gain access to the required data. These treaties will facilitate international judicial cooperation in solving criminal cases.
- Assuring the proper technical means and specialized personnel for enforcement of surveillance warrants obtained by Directorate of Special Operations of Romanian Police Department
- Acquisition and/or development of specialized software for decrypting intercepted data obtained from mobile operators and ISPs

3. Conclusions

Criminal activities are and will always be up to date with latest technological discoveries and equipment. In this context, the reaction of criminal law enforcement bodies must be firm. Law enforcements efficiency greatly depends on access to technology. The legislature has now provided the legal framework that sets out the conditions in which they can issue warrants for surveillance technique that include conversations via the internet. To be effective and provide evidence surveillance warrants must be enforced in a very short term.

References

1. Mihail Udroiu – *Code of Criminal Procedure. General Part, New Code of Criminal Procedure*, C.H. Beck Publishing House, page 308.
2. Adrian Petre, Catalin Grigoras - *Audio and audio-video recordings*, C.H. Beck Publishing House, Bucharest 2010
3. Mihail Udroiu, R. Slavoiu, O. Predescu - *Special investigative techniques in criminal justice*, C.H. Beck Publishing House, Bucharest 2009
4. Mihai Viorel Tudoran - *Theory and practice of audio and video interception*, Universul Juridic Publishing House, Bucharest 2012
5. N.Volonciu, A. Barbu - *Commented Code of Criminal Procedure, Articles 62-135. Samples and evidence*, Hamangiu Publishing House, Bucharest, 2007
Legislation
Romania Code of Criminal Procedure
Romania Criminal Code (offenses provided in Article 226, Article 302, Article 324, Article 361
Law No 51/1991 on Romania's national security.
Law No 535/2004 on preventing and combating terrorism.
Law No 191/1998 the organization and functioning of the Security and Protection Service
Law No 143/2000 -Law against illicit drug trafficking
Law No 678/2001 on preventing and combating trafficking in persons
Law No 39/2003 on preventing and combating organized crime.
Law No 656/2002 on preventing money laundering
Law No 78/2000 on preventing, discovering and sanctioning corruption

INTERCEPTION OF COMMUNICATIONS MADE OVER THE INTERNET IN ACCORDANCE WITH THE PROVISIONS OF THE CODE OF CRIMINAL PROCEDURE

Law No 64 / 2004 for putting in effect the Council's of Europe Convention on Cybercrime
Law No 591/2002 - Law approving Government Emergency Ordinance No. 79/2002 on the general regulatory framework for communications
Law No 506/2004 regarding the processing of personal data and privacy in the electronic communications sector
Websites
1. http: //verint.com/services/index.html
2. www.wikipedia.com

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number **POSDRU/159/1.5/S/138822** with the title ***"Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers - "SmartSPODAS"."***